UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/868,417	10/23/2001	Charles Cameron Lindquist	12143/1	1411

26646 7590 05/21/2007

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
MEUCCI, MICHAEL D	
ART UNIT	**PAPER NUMBER**
2142	

MAIL DATE	DELIVERY MODE
05/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/868,417	LINDQUIST, CHARLES CAMERON	
	Examiner	Art Unit	
	Michael D. Meucci	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *59-120* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *59-120* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the request for reconsideration filed on 12 March 2007.

2. Claims 59-120 remain pending.

Claim Objections

3. Claim 60 objected to because of the following informalities: remove "in" after "wherein" on line 1 of the claim. Appropriate correction is required.

4. Claim 108 objected to because of the following informalities: "smart card" should be replaced with --smartcard-- of the claim and remain consistent throughout the claims. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 89 and 109-116 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Claim 89 recites the limitation "said network" in line 8, "the establishment of a network" in line 9, "the temporary interconnection" on line 10. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

8. Claims 59-64, 67, 71, 72, 75, 88-94, 100-102, 109-118, and 120 rejected under 35 U.S.C. 102(a) as being anticipated by Venkatraman et al. (EP 0 838 768 A2) hereinafter referred to as Venkatraman.

a. As per claim 59, Venkatraman teaches: an Internet browser connectable to an extranet (lines 24-29 of page 2); an extranet located external to said environment and accessible via said Internet browser (line 37 of page 4 through line 1 of page 5 and Fig. 2); a communications server located in said extranet and adapted to interconnect on demand with one of a series of connection gateways located in predetermined environments (lines 38-43 of page 2, lines 24-40 of page 4, and item 30 in Fig. 2; wherein cellular transmitter/receiver circuitry inherently contains on-demand connectivity features); a connection gateway located in said environment to server as a user interface for the control or monitoring of the operation of at least one service in said environment (lines 15-18 of page 4, lines 30-33 of page 4, lines 37-40 of page 4, and item 30 in Fig. 2); wherein upon accessing a predetermined address by said Internet browser on said extranet, said communications server creates a new connection to a predetermined one of said connection gateways to control or monitor the operation of said service, with said connection gateway subsequently serving pages directly to said

internet browser displaying the state of operation of said service (lines 14-24 of page 3 and lines 6-12 of page 5).

b. As per claim 60, Venkatraman teaches: wherein the connection gateway located in said environment is adapted to serve a user interface for the control or monitoring of the operation of at least one service in said environment (lines 24-29 of page 2).

c. As per claims 61 and 62, Venkatraman teaches: said service is adapted to monitor and control, one or more devices interconnected with said connection gateway (lines 24-29 of page 2).

d. As per claim 63, Venkatraman teaches: wherein at least one of said devices is a monitoring device located within said environment (lines 8-9 of page 2 and lines 37-40 of page 6).

e. As per claim 64, Venkatraman teaches: said communication server utilizes a telecommunications network to interconnect with said connection gateway (lines 44-45 of page 3).

f. As per claim 67, Venkatraman teaches: publicly accessible HTML pages are additionally provided for each user of said system providing details of the current status of the environment of said user (lines 52-55 of page 2 and lines 28-36 of page 3).

g. As per claims 71 and 118, Venkatraman teaches: the Internet access device is a computer, WebPhone, portable digital assistant, or mobile phone with web browsing capability; and the internet browser is on a mobile phone (line 37 on page 3 through line 1 of page 4 and lines 45-55 of page 4).

h. As per claim 72, Venkatraman teaches: wherein the connection gateway detects a fax and stores the fax (lines 5-11 of page 2).

i. As per claim 75, Venkatraman teaches: wherein the connection gateway acts as a hub and Internet connection mechanism for connected devices including information appliances and said devices located in said environment (lines 5-11 of page 2).

j. As per claim 88, Venkatraman teaches: wherein said connection gateways form nodes of a distributed computing environment that may be allocated by said extranet on a demand basis (lines 35-36 of page 4).

k. As per claim 89, Venkatraman teaches: extranet is a first network having a first network controller (line 37 of page 4 through line 1 of page 5 and Fig. 2); environment is a second network having a second network access controller (lines 15-18 of page 4, lines 30-33 of page 4, lines 37-40 of page 4, and item 30 in Fig. 2); a user access browser located on said first network for locating and examining information on said first and second networks by means of network address locators (line 37 of page 4 through line 1 of page 5 and Fig. 2); wherein when a predetermined location on said network is accessed, said first network access controller initiates the establishment of a network connection to said second network access controller so as to provide for the temporary interconnection of said first network to said second network, said system thereby providing a seamless access to information stored on said second network from said user access browser (lines 14-24 of page 3 and lines 6-12 of page 5).

l. As per claim 90, Venkatraman teaches: network address locators comprise Universal Resource Locators (lines 33-36 of page 3).

m. As per claim 91, Venkatraman teaches: storage means forming part of said extranet (lines 34-36 of page 4); a device activating a security condition upon the occurrence of a predetermined event (lines 37-40 of page 6); wherein, upon the occurrence of said predetermined event, said device notifies said connection gateway and transfers event information on said predetermined event to said connection gateway and said connection gateway establishes an interconnection with said communications server and transfers said event information via said communications server to said storage means for later interrogation by a user of said system and initiates predetermined alert notification actions (lines 31-36 of page 6).

n. As per claim 92, Venkatraman teaches: wherein said device includes alert conditions which are forwarded to said connection gateway, wherein it is qualified with a pre-programmed enable, and if the result is TRUE, an event is generated, whereupon said connection gateway establishes a connection with one of said communications servers (lines 37-40 of page 6).

o. As per claim 93, Venkatraman teaches: wherein said device is a security sensor device, said system is a security system, said event is a security alarm event, and said data is surveillance data or security alert data (lines 45-45 of page 4 and lines 31-36 of page 6).

p. As per claim 94, Venkatraman teaches: wherein surveillance data related to said alarm event is uploaded to said extranet for secure storage accessible upon interrogation by a user (lines 33-36 of page 6).

q. As per claim 96, Venkatraman teaches: wherein the connection gateway incorporates a user programmed phone call answer strategy, including delayed answer, and upon answering said phone call, optionally detects a voice call, in which case it records a compressed version of the voice call for later retrieval by the user, thus operating in answering machine mode (lines 43-47 of page 3).

r. As per claim 97, Venkatraman teaches: wherein upon answering an incoming call, the connection gateway raise a connection to a communications server, and sends an indication to the user of said security system of the receipt of a recorded message (lines 43-47 of page 3).

s. As per claim 98, Venkatraman teaches: wherein said connection gateway sends a recorded compressed voice messages to a communications server for storage on said extranet for forwarding to a user of said environment (lines 43-47 of page 3).

t. As per claim 99, Venkatraman teaches: wherein the connection gateway provides an indication of massages received on a HTML page accessible by a user of said home environment (lines 28-32 of page 3).

u. As per claim 100, Venkatraman teaches: wherein said connection gateway is programmable to allow different response mechanisms to differing classes of alert events (lines 21-36 of page 6).

v. As per claim 101, Venkatraman teaches: wherein said connection gateway contains connection details for preferred and secondary communication servers on said extranet, so that if a first communication server does not respond, other communication servers may be contacted until successful connection is achieved (lines 34-36 of page 3).

w. As per claim 102, Venkatraman teaches: wherein user data storage on said extranet for storing event data associated with said environment is allocated virtually (lines 34-36 of page 4).

x. As per claim 104, Venkatraman teaches: wherein said extranet includes a user contact database which includes preferred contact methods, allowing automatic contact mechanisms to be associated with alarm condition, including use of email, page, computer generated voice message through telephone, requesting response, or after a specified timeout has elapsed, security action (lines 41-44 of page 4).

y. As per claim 105, Venkatraman teaches: wherein at least one of said devices includes an external access control mechanism to said environment (lines 43-45 of page 3).

z. As per claims 109-116, Venkatraman teaches: wherein said environment is a home environment, a commercial environment, or industrial environment; the at least one service includes a security monitoring service; the at least one service includes a video surveillance service; the at least one service includes an automation and control service; the at least one service includes a utility metering service; and the at least one service includes an energy management service (page 2).

aa. As per claim 117 and 120, Venkatraman teaches: the at least one service implements monitoring or control of a plurality of devices connected to at least one network interconnected with the connection gateway; and the connection gateway is embodied in a security camera (lines 37-53 of page 3).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 66, 68, 73, 74, 83, 85-86, and 103 rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatraman as applied to claims 59 and 92 above.

a. As per claim 66, Venkatraman does not explicitly teach: said extranet forms part of the Internet and said communications server is located within the local telephone call radius of the environment, thus providing lower cost PSTN access from or to the environment. However, Official Notice is taken of communication servers being located within the local telephone call radius of the environment. Internet service providers for dial-up internet services have long set up local telephone access numbers such that the customer does not pay for long-distance telephone calls. This concept is extremely well known in the art.

b. As per claim 68, Venkatraman does not explicitly teach: wherein said extranet provides a user premises e-mail facility, and automatically raises connection in

a pre-programmed fashion to said connection gateway and transfers user e-mail to said connection gateway. However, Official Notice is taking of automatically connecting to and sending user e-mail to the connection gateway. Users composing e-mail offline are prompted to connect to the network when attempting to send emails while offline. This feature was common in Eudora email systems as well as many others years ago. As such this concept is extremely well know in the art.

c. As per claims 73-74, Venkatraman does not explicitly teach: the connection gateway is in a tamper-proof enclosure, and operates without main power; and the connection gateway is tamper-proof and triggers an alarm and relays alarm to the provider network in case of attempted tampering. However, Official Notice is taken of these features. Both are extremely well known in the art and can be found in/on many security systems.

d. As per claim 83, Venkatraman does not explicitly teach: the control terminal includes a set top box connected to a television and executes a web browser. However, Official Notice is taken of this feature. This limitation is extremely well known in the art and has been implemented in many systems for many years.

e. As per claims 85-86, Venkatraman teaches: a digital security camera having interconnection to said connection gateway (lines 2-8 of page 4).

Venkatraman does not explicitly teach: the digital security camera having an image capture and compression functionality; and said camera includes motion detection and image significance algorithms which run in said camera, and filter input so that only detected motion input is compressed and sent through said connection

gateway to said extranet. However, Official notice is taken of a camera having image capture and compression functionality, as well as motion detection, image significance algorithms, and filtering input. These limitations are extremely well known in the art and have been made and used in security systems for many years.

f. As per claim 103, Venkatraman does not explicitly teach: wherein said user data storage on said extranet is allocated redundantly, ensuring integrity of stored surveillance data. However, Official Notice is taken of storing and allocating data redundantly because it has been very well known in the art for years. Evidence can be found in RAID systems levels 1-5 defined in 1988. It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have user data storage on the extranet allocated redundantly in the system as taught by Venkatraman.

11. Claims 65 rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatraman as applied to claim 59 above, in view of Buffam (U.S. 6,185,316 B1).

a. As per claim 65, Venkatraman does not explicitly teach: authentication to access said extranet is required only once per Internet browser session. However, Buffam discloses: "To address the problems described above, login authentication schemes have been developed that only require users to authenticate once during a session," (lines 22-24 of column 5). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to authenticate access said extranet only once per Internet browser session. "These approaches are commonly referred to

as unitary login, or single sign-on. Unitary login is generally a two-step process, in which the user first authenticates to a user using, for example, a password, token, or biometric sample. The principal may be the user's workstation, a physical authentication token, or some other device. Then, as the user requests access to various services, the principal is responsible for authenticating the user to each service," (lines 24-32 of column 5 in Buffam). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to authenticate access said extranet only once per Internet browser session in the system as taught be Venkatraman.

12. Claims 69, 70, 84, 106, 107, and 119 rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatraman as applied to claim 59, in view of Chen et al. (U.S. 5,784,463) hereinafter referred to as Chen.

a. As per claims 69 and 119, Venkatraman teaches: a URL corresponding to said environment (lines 20-24 of page 3). Venkatraman does not explicitly teach: the Internet browser runs on an Internet access device which includes a smart card reader and associated user smart card which provides authentication details; and at least one of said devices includes a reader for an RF tag embodied in keyfob or other device that is used for user authentication. However, Chen discloses: "It will be appreciated that the tokens used by the present invention may take a variety of forms, and that the term "token" is intended to refer to any device capable of sending and receiving challenges and responses during a user authentication process, including but not limited to smartcards and PCMCIA cards, or software on a user's computer, and that the term

"reader" is intended to refer to any device capable of transmitting data to and from a token. Numerous different types of tokens are currently available, and the invention is intended to be compatible with all such devices," (lines 6-16 of column 4). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have a smart card and reader for authentication purposes; and have at least one of said devices include a reader for an RF tag embodied in keyfob or other device that is used for user authentication. "It will also be appreciated by those skilled in the art that the invention is not limited to any particular browser or application software, but rather that the invention can be use with any applications supported by the server," (lines 16-20 of column 4 in Chen). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have a smart card and reader for authentication; and at least one of said devices include a reader for an RF tag embodied in keyfob or other device that is used for user authentication in the system as taught by Venkatraman.

b. As per claims 70 and 84, Venkatraman does not explicitly teach: wherein said smart card also facilitates global access to the Internet for access of said extranet, and optionally additionally tracks connections for expensing. However, Chen discloses: "The preferred embodiment of the invention is practiced on a communications network 5 such as the Internet, made up of client nodes 10, each of which is connected to at least one computing device capable reading a "token", (lines 4-7 of column 4). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have said smart card also facilitate global access to the Internet for access of said

extranet, and optionally additionally track connections for expensing. "It will be appreciated that the tokens used by the present invention may take a variety of forms, and that the term "token" is intended to refer to any device capable of sending and receiving challenges and responses during a user authentication process, including but not limited to smartcards and PCMCIA cards, or software on a user's computer, and that the term "reader" is intended to refer to any device capable of transmitting data to and from a token. Numerous different types of tokens are currently available, and the invention is intended to be compatible with all such devices. It will also be appreciated by those skilled in the art that the invention is not limited to any particular browser or application software, but rather that the invention can be use with any applications supported by the server," (lines 7-20 of column 4 in Chen). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have said smart card also facilitate global access to the Internet for access of said extranet, and optionally additionally track connections for expensing in the system as taught by Venkatraman.

13. Claims 76 and 78-82 rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatraman as applied to claim 59 above, in view of Moon et al. (U.S. 6,433,801 B1) hereinafter referred to as Moon.

a. As per claim 76, Venkatraman teaches: a control terminal interconnected to said connection gateway, said control terminal comprising a display and a running web browser (lines 24-29 of page 2).

Venkatraman does not explicitly teach: the display incorporating a touch screen. However, Moon discloses: "It is yet a further object of the present invention to provide a portable intelligent communications device that includes a cellular telephone and a touch screen display," (lines 21-23 of column 2). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have a touch screen display. "A touch screen display which is capable of moving and automatically naming tabbed control panels based upon control names," (lines 23-25 of column 2 in Moon). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have a touch screen display in the system as taught by Venkatraman.

b. As per claim 78-80, Venkatraman teaches: the control terminal is connected to said connection gateway in a wireless manner; the control terminal is powered by rechargeable batteries, allowing the control terminal mobility within the range of wireless transmitters attached to the user premises network in said environment; and the control terminal is of reduced handheld size, so that it can operate as a universal premises remote control (lines 43-47 of page 3).

c. As per claim 81, Venkatraman teaches: the control terminal includes a digital camera, microphone and speaker, and video conferencing software, thus allowing the control terminal to be used as a videophone, through a standard browser interface (lines 2-8 of page 4).

d. As per claim 82, Venkatraman teaches: the control terminal includes a personal computer (PC) equipped with a user premises network connection, wherein

said PC runs a browser accessing a URL corresponding to said connection gateway (page 3).

14. Claims 77 and 108 rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatraman as applied to claims 76 and 107 above, in view of Foster, Jr. (U.S. 5,668,929) hereinafter referred to as Foster.

a. As per claim 77, Venkatraman does not explicitly teach: the control terminal is equipped with a biosensor, for access authentication of a local user in said environment to said connection gateway. However, Foster discloses: "In that regard, the present invention security devices and systems may be used alone or together with other forms of security, such as by way of example, a card reader, biological sensors of some kind such as a fingerprint sensor, eye separation detector, photo recording and/or verification or other facial or facial feature recognition (automatic or through a remotely located security officer), etc., or even some level of voice recognition," (lines 56-63 of column 4). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include a biosensor for user authentication. "Security devices and systems may be used alone or together with other forms of security," (lines 57-58 of column 4 in Foster). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to include a biosensor for user authentication.

b. As per claim 108, Venkatraman does not explicitly teach: wherein the smartcard includes a biosensor attached to the substrate of the smart card and

interconnected with a circuit embedded in smartcard to authenticate user before the smartcard will operate. However, Foster discloses: "In that regard, the present invention security devices and systems may be used alone or together with other forms of security, such as by way of example, a card reader, biological sensors of some kind such as a fingerprint sensor, eye separation detector, photo recording and/or verification or other facial or facial feature recognition (automatic or through a remotely located security officer), etc., or even some level of voice recognition," (lines 56-63 of column 4). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have the smartcard include a biosensor attached to the substrate of the smart card and interconnected with a circuit embedded in smartcard to authenticate user before the smartcard will operate. "Security devices and systems may be used alone or together with other forms of security," (lines 57-58 of column 4 in Foster). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have the smartcard include a biosensor attached to the substrate of the smart card and interconnected with a circuit embedded in smartcard to authenticate user before the smartcard will operate in the system as taught by Venkatraman.

15. Claim 87 rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatraman as applied to claim 59 above, in view of Lea et al. (U.S. 6,032,202) hereinafter referred to as Lea.

a. As per claim 87, Venkatraman does not explicitly teach: the connection gateway provides support for at least one of HomePnP, Bluetooth, HomeRF, Hiperlan, and HAVi standards for network communication and appliance control. However, Lea discloses: "Specifically, the HAVI architecture provides: an execution environment supporting the visual representation and control of appliances; application and system services; and communication mechanisms for extending the environment dynamically through plug and play or otherwise," (lines 17-21 of column 6). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include at least one of these protocols. "It should be noted that the HAVI architecture supports legacy appliances (e.g., appliances that already exist and are available to users). This is important since the transition to more intelligent networked appliances is going to be slow. Most manufacturers will not suddenly begin producing only "intelligent" appliances and most consumers will not quickly begin replacing all of their existing appliances," (lines 22-29 of column 6 in Lea). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to include at least one of these protocols in the system as taught by Venkatraman.

16. Claim 95 rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatraman as applied to claim 92 above, in view of Conklin et al. (U.S. 5,991,881) hereinafter referred to as Conklin.

a. As per claim 95, Venkatraman does not explicitly teach: wherein photos of authorized occupants of said environment are accessible from said extranet and are

accessed upon said alarm event and cross referenced with said surveillance data to ascertain whether a true alarm condition has been raised. However, Conklin discloses: "The system operates to monitor and control sensors and actuators, handles event logging, generates alarm maps and related displays, and switches and distributes surveillance video," (lines 19-23 of column 2). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have photos of authorized occupants of said environment accessible from said extranet and accessed upon said alarm event and cross referenced with said surveillance data to ascertain whether a true alarm condition has been raised. "The system described will generally use the existing complement of sensors and actuators as included in an existing intrusion subsystem, existing video surveillance equipment, and the existing voice and data communication subsystems. The present invention operates to integrate the operation so that these separate subsystems can be conveniently monitored by a single console to enable a single operator to monitor and therefore control the various subsystems of concern," (lines 23-32 of column 2 in Conklin). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have photos of authorized occupants of said environment accessible from said extranet and accessed upon said alarm event and cross referenced with said surveillance data to ascertain whether a true alarm condition has been raised in the system as taught by Venkatraman.

Response to Arguments

17. Applicant's arguments filed 12 March 2007 have been fully considered but they are not persuasive.

18. (A) Regarding claim 59, the applicant contends that Venkatraman does not teach: wherein upon accessing a predetermined address by said Internet browser on said extranet, said communications server creates a new connection to a predetermined one of said connection gateways to control or monitor the operation of said service, with said connection gateway subsequently serving pages directly to said internet browser displaying the state of operation of said service. The examiner respectfully disagrees.

As to point (A), the applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. The examiner points out that the entire specification of Venkatraman is an enabling disclosure of the argued limitation. Sections of Venkatraman clearly disclose: accessing a predetermined address on the extranet (lines 20-21 on page 3) by an internet browser (line 10 on page 5), the communications server creating a new connection to one of the predetermined gateways (lines 37-40 of page 6), wherein the gateway provides access to information contained within the environment directly to the browser (lines 31-35 of page 6). The examiner can provide no further evidence towards the argued limitation because

Venkatraman is so explicit in teaching this limitation. As such, the rejection remains proper and is maintained by the examiner.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Elliott (U.S. 7,145,898 B1) discloses selection of gateways for hybrid communication systems.

Kumaki et al. (U.S. 7,151,758 B2) discloses communication handoff control for mobile terminals.

Khuc (U.S. 2006/0203809 A1) discloses an internet routing system and gateways.

Blumenau (U.S. 2007/0106792 A1) discloses monitoring browser access.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Meucci at (571) 272-3892. The examiner can normally be reached on Monday-Friday from 9:00 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell, can be reached at (571) 272-3868. The fax phone number for this Group is 571-273-8300.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [michael.meucci@uspto.gov].

All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beatriz Prieto

BEATRIZ PRIETO
PRIMARY EXAMINER